University of Ottawa

Department of Mathematics and Statistics

MAT 3143: Ring Theory

Professor: Alistair Savage

Final Exam – Solutions

April 2018

Surname _____ First Name _____

Student # _____

Instructions:

(a) You have 3 hours to complete this exam.
(b) Unless otherwise indicated, you must justify your answers to receive full marks.
(c) Write your student number at the top of each page in the space provided.
(d) You may use the last page of the exam as scrap paper.

Mobile phones, unauthorized electronic devices or course notes are not allowed during this exam. Phones and devices must be turned off and put away in your bag. Do not keep them in your possession, such as in your pockets. If caught with such a device or document, the following may occur: academic fraud allegations will be filed which may result in your obtaining a 0 (zero) for the exam.

By signing below, you acknowledge that you have read and ensured that you are complying with the above statement.

Signature: _____

Good luck!

Please do not write in the table below.

Question	1	2	3	4	5	6	7	8	9	10	11	12	Total
Maximum	3	3	3	3	3	4	4	6	7	5	3	3	47
Grade													

QUESTION 1. Give an example of each of the following. You should justify that your example satisfies the given requirements.

(a) **[1 point]** An idempotent element of the ring $M_n(\mathbb{R})$ of $n \times n$ real matrices, $n \geq 2$, that is neither the zero matrix nor the identity matrix. Do *not* choose a specific value for n. (That is, give an answer for each $n \geq 2$.)

Solution: Suppose $n \geq 2$. Then the matrix

$$M = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

is an idempotent since $M^2 = M$. Clearly M is neither the zero matrix nor the identity matrix (since $n \geq 2$). Of course, there are other possible answers.

(b) **[1 point]** A field extension of $\mathbb{Q}$ of degree n, $n \geq 2$. Do *not* choose a specific value for n. (That is, give an answer for each $n \geq 2$.)

Solution: Suppose $n \geq 2$. Then $x^n - 2$ is irreducible by the Eisenstein criterion with $p = 2$. Hence $\langle x^n - 2 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$. Thus $\mathbb{Q}[x]/\langle x^n - 2 \rangle$ is a field extension of $\mathbb{Q}$ of degree n.

(c) **[1 point]** A pair of rings $R \subseteq S$ and an element a that is irreducible in S but is not irreducible in R.

Solution: Take $R = \mathbb{Z}[x]$, $S = \mathbb{Q}[x]$, and $a = 2x$. Then a is irreducible in $\mathbb{Q}[x]$ since it is linear and $\mathbb{Q}$ is a field. However, in $\mathbb{Z}[x]$, a is a product of the nonunits 2 and x. Hence a is not irreducible in $\mathbb{Z}[x]$.

QUESTION 2. **[3 points]** Suppose that $\theta\colon R \to S$ is a ring homomorphism such that $\theta(R)$ and $\ker\theta$ both contain no nonzero nilpotent elements. Show that R contains no nonzero nilpotent elements.

Solution: Suppose that $\theta(R)$ and $\ker\theta$ both contain no nonzero nilpotent elements. Let r be a nilpotent element of R. Thus $r^n = 0$ for some $n \in \mathbb{N}$. Therefore

$$\theta(r)^n = \theta(r^n) = \theta(0) = 0.$$

Since $\theta(R)$ has non nonzero nilpotent elements, this implies that $\theta(r) = 0$, and so $r \in \ker\theta$. But since $\ker\theta$ has no nonzero nilpotent elements, we must have $r = 0$. Hence zero is the only nilpotent element of R.

QUESTION 3. Consider the polynomial

$$f(x) = x^3 + 16x + 6.$$

(a) **[1 point]** Is $f(x)$ irreducible over $\mathbb{Q}$? Remember to justify your answer.

Solution: Yes, it is irreducible over $\mathbb{Q}$ by the Eisenstein criterion with $p = 2$.

(b) **[1 point]** Is $f(x)$ irreducible over $\mathbb{Z}_3$? Remember to justify your answer.

Solution: In $\mathbb{Z}_3[x]$, we have $f(x) = x^3 + x = x(x^2 + 1)$, and so f is not irreducible over $\mathbb{Z}_3$. (You can also note that $f(0) = 0$ in $\mathbb{Z}_3$.)

(c) **[1 point]** Is $f(x)$ irreducible over $\mathbb{Z}_5$? Remember to justify your answer.

Solution: In $\mathbb{Z}_5[x]$, we have $f(x) = x^3 + x + 1$. Since

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 1, \quad f(3) = 1, \quad f(4) = 4,$$

and $\deg f = 3$, we see that f is irreducible over $\mathbb{Z}_5$.

QUESTION 4. **[3 points]** Let

$$A = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N},\ a_0 \in 5\mathbb{Z},\ a_1, \ldots, a_n \in \mathbb{Z}\}$$

Prove that A is an ideal of $\mathbb{Z}[x]$ and that $\mathbb{Z}[x]/A \cong \mathbb{Z}_5$ (isomorphism of rings).

Solution: Consider the composition of ring homomorphisms

$$\theta\colon \mathbb{Z}[x] \xrightarrow{\varphi_0}\!\!\rightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/5\mathbb{Z},$$

where the first homomorphism is evaluation at zero and the second is the canonical projection $m \mapsto m + 5\mathbb{Z}$, $x \in \mathbb{Z}$. Then $\ker\theta = A$, and so A is an ideal of $\mathbb{Z}[x]$. For any $m \in \mathbb{Z}$, we have $\theta(m) = m + 5\mathbb{Z}$, and so θ is surjective. Thus, it follows from the First Isomorphism Theorem that $\mathbb{Z}[x]/A \cong \mathbb{Z}_5$ as rings.

QUESTION 5. **[3 points]** Suppose R is an integral domain. Prove that if $R[x]$ is a PID, then R is a field. *Hint*: Suppose $R[x]$ is a PID and choose a nonzero element $a \in R$. Use the fact that the ideal $\langle a, x\rangle$ is principal to show that a is a unit.

Solution: Suppose $R[x]$ is a PID, and let $a \in R \setminus \{0\}$. Then $\langle a, x\rangle = \langle f\rangle$ for some $f \in R[x]$. Since $a \in \langle a, x\rangle$, we thus have $a = fg$ for some $g \in R[x]$. Thus $\deg f = 0$. So f is a constant polynomial, that is, $f \in R$.

Since $x \in \langle a, x\rangle$, we have $x = fh$ for some $h \in R[x]$. Since $f \in R$, we have $\deg h = 1$, so that $h = bx + c$ for some $b, c \in R$. Then

$$x = fh = (fb)x + fc,$$

which implies that $fb = 1$. So f is a unit, and hence $\langle a, x\rangle = \langle f\rangle = R[x]$. In particular, there exists $p, q \in R[x]$ such that $1 = ap + qx$. Evaluating at $x = 0$, we have $1 = ap(0)$. In particular, a is a unit in R.

QUESTION 6. Let $p = 2 + \sqrt{-5} \in \mathbb{Z}(\sqrt{-5})$.

(a) **[2 points]** Show that p is irreducible in $\mathbb{Z}(\sqrt{-5})$.

Solution: Suppose $p = (a + b\sqrt{-5})(c + d\sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}$. Then we have

$$(a^2 + 5b^2)(c^2 + 5d^2) = N(p) = 2^2 + 5 = 9.$$

Since there are no integers a, b such that $a^2 + 5b^2 = 3$, we have, without loss of generality, $a^2 + 5b^2 = 1$, which implies that $b = 0$ and $a = \pm 1$. Hence $a + b\sqrt{-5} = \pm 1$ is a unit in $\mathbb{Z}(\sqrt{-5})$. Therefore p is irreducible.

(b) **[2 points]** Show that p is not prime in $\mathbb{Z}(\sqrt{-5})$.

Solution: Note that

$$(2 + \sqrt{-5})(2 - \sqrt{-5}) = 2^2 + 5 = 9 = 3 \cdot 3.$$

We claim that p does not divide 3, from which it follows that p is not prime. Indeed, if p divided 3, there would exist $a, b \in \mathbb{Z}$ such that

$$(2 + \sqrt{-5})(a + b\sqrt{-5}) = 3,$$

which implies that

$$9 = N(3) = N(2 + \sqrt{-5})N(a + b\sqrt{-5}) = 9(a^2 + 5b^2).$$

This implies that $a^2 + 5b^2 = 1$ and so $b = 0$, $a = \pm 1$. However, $p \neq \pm 3$, yielding a contradiction.

QUESTION 7.

(a) **[1 point]** Give the definition of a *euclidean domain*.

Solution: An integral domain R is called a euclidean domain if there is a function $\nu\colon R \setminus \{0\} \to \mathbb{N}$ such that

$$a, b \in R \setminus \{0\} \implies \nu(ab) \geq \nu(a),$$

and such that, for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with

$$a = qb + r \text{ and either } r = 0 \text{ or } \nu(r) < \nu(b).$$

(b) **[3 points]** Prove that every euclidean domain is a PID.

Solution: Suppose R has a euclidean valuation ν, and let I be an ideal of R. If I is the zero ideal, then it is clearly principal. So we assume $I \neq \{0\}$. Choose $b \in I \setminus \{0\}$ with $\nu(b)$ minimal. We claim that $I = \langle b \rangle$. Since $b \in I$, we have $\langle b \rangle \subseteq I$. So it remains to show that $I \subseteq \langle b \rangle$. Suppose $a \in I$. Then we have

$$a = qb + r \quad \text{where } r = 0 \text{ or } \nu(r) < \nu(b).$$

Then $r = a - bq \in I$ and so, by the minimality of $\nu(b)$, we must have $r = 0$. Thus $a = qb$ and so $a \in \langle b \rangle$.

QUESTION 8.

(a) **[2 points]** Let R be a ring. Suppose that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is an infinite chain of ideals of R. Prove that $\bigcup_{n=1}^{\infty} I_n$ is an ideal of R.

(b) **[1 point]** If I and J are ideals of a ring R, it is necessarily true that $I \cup J$ is an ideal of R? Remember to justify your answer.

(c) **[1 point]** State the ACCP for integral domains.

(d) **[2 points]** Prove that every PID satisfies the ACCP.

Solution:

(a) Let $I = \bigcup_{n=1}^{\infty} I_n$. Since $0 \in I_1$, we have $0 \in I$. Suppose $a, b \in I$. Then $a \in I_n$ for some n and $b \in I_m$ for some m. Let $k = \max\{n, m\}$. Then $a, b \in I_k$. Since I_k is an ideal, we have $a - b \in I_k \subseteq I$. Hence I is an additive subgroup of R.

Now suppose $a \in I$ and $r \in R$. Then $a \in I_n$ for some n. Since I_n is an ideal, we have $ra, ar \in I_n \subseteq I$. Hence $RI, IR \subseteq I$. So I is an ideal of R.

(b) No, $I \cup J$ is not necessarily an ideal of R. For example, consider $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, and $J = 3\mathbb{Z}$. Then $2, 3 \in I \cup J$, but $2 + 3 = 5 \notin I \cup J$.

(c) An integral domain R satisfies the *ascending chain condition on principal ideals* (or *ACCP*) if R contains no strictly increasing infinite chain

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$$

of principal ideals.

(d) Suppose R is a PID. Suppose, towards a contradiction, that R contains a strictly increasing infinite chain

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$$

of principal ideals. By part (a), $I = \bigcup_{n=1}^{\infty} \langle a_n \rangle$ is an ideal of R. Since R is a PID, we have $I = \langle b \rangle$ for some $b \in R$. Then $b \in \langle a_n \rangle$ for some n, which implies that $I \subseteq \langle a_n \rangle$. Since we clearly have $\langle a_n \rangle \subseteq I$, it follows that $\langle a_n \rangle = I$. But this contradicts the assumption that $\langle a_n \rangle \subsetneq \langle a_{n+1} \rangle \subseteq I$.

QUESTION 9. Suppose $F \subseteq E$ is a field extension and let $u, v \in E$ be algebraic over F of degrees m, n (respectively).

(a) **[2 points]** Show that $[F(u,v) : F] \leq mn$.

(b) **[2 points]** Show that, if m and n are relatively prime, then $[F(u,v) : F] = mn$.

(c) **[3 points]** Is the converse to (b) true? Justify your answer.

Solution:

(a) Consider the chain of fields $F \subseteq F(u) \subseteq F(u,v)$. By the Multiplication Theorem, we have $[F(u,v) : F] = [F(u,v) : F(u)][F(u) : F]$. Let f be the minimal polynomial of v over F, so that $\deg f = \deg_F v$. Since $f(v) = 0$, the minimal polynomial of v over $F(u)$ must divide f in $F(u)[x]$. So $[F(u,v) : F(u)] = \deg_{F(u)} v \leq \deg f = [F(v) : F]$. Therefore, we have

$$[F(u,v) : F] = [F(u,v) : F(u)][F(u) : F] \leq [F(v) : F][F(u) : F] = nm.$$

(b) Consider the chains of fields

$$F \subseteq F(u) \subseteq F(u,v) \quad \text{and} \quad F \subseteq F(v) \subseteq F(u,v).$$

By the Multiplication Theorem, we have

$$[F(u,v) : F] = [F(u,v) : F(u)][F(u) : F] \quad \text{and} \quad [F(u,v) : F] = [F(u,v) : F(v)][F(v) : F].$$

In particular m and n both divide $[F(u,v) : F]$. Thus $mn = \operatorname{lcm}(m,n)$ divides $[F(u,v) : F]$, and so $mn \leq [F(u,v) : F]$. Combined with the result from (a), this shows that $[F(u,v) : F] = mn$.

(c) No, the converse is false. For example, consider $F = \mathbb{Q}$ and $E = \mathbb{C}$, $u = \sqrt{2}$, and $v = \sqrt{-1}$. Then we have a chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{-1}).$$

Since $x^2 - 2$ is irreducible over $\mathbb{Q}$ (by the Eisenstein criterion with $p = 2$), we have

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Then note that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\sqrt{-1} \notin \mathbb{R}$. Hence $[\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}(\sqrt{2})] \geq 2$. Since $\sqrt{-1}$ is a root of $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$, we also have $[\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}(\sqrt{2})] \leq 2$. So $[\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}(\sqrt{2})] = 2$, and hence

$$[\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

We also have $[\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = 2$, since the minimal polynomial of $\sqrt{-1}$ over $\mathbb{Q}$ is $x^2 + 1$. Thus

$$[\mathbb{Q}(\sqrt{2}, \sqrt{-1}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}].$$

However, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ and $[\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}]$ are not relatively prime.

QUESTION 10. Consider the polynomial $f(x) = x^3 - 7$.

(a) **[1 point]** Find the splitting field E of $f(x)$ over $\mathbb{Q}$.

(b) **[4 points]** What is $[E : \mathbb{Q}]$? Give a basis for E over $\mathbb{Q}$.

Solution:

(a) We have

$$x^3 - 5 = (x - \sqrt[3]{7})(x - \omega\sqrt[3]{7})(x - \omega^2\sqrt[3]{7}), \quad \omega = e^{2\pi i/3}.$$

So $E = \mathbb{Q}(\sqrt[3]{7}, \omega\sqrt[3]{7}, \omega^2\sqrt[3]{7}) = \mathbb{Q}(\sqrt[3]{7}, \omega)$.

(b) Consider the extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{7}) \subseteq \mathbb{Q}(\sqrt[3]{7}, \omega).$$

Since $x^3 - 7$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion with $p = 7$, we have

$$[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = \deg(x^3 - 7) = 3.$$

Since $\mathbb{Q}(\sqrt[3]{7}) \subsetneq \mathbb{Q}(\sqrt[3]{7}, \omega)$, we have

$$2 \leq [\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}(\sqrt[3]{7})] = \deg m(x), \tag{1}$$

where $m(x)$ is the minimal polynomial of ω in $\mathbb{Q}(\sqrt[3]{7})[x]$. Now, ω is a root of

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

Since ω is not a root of the first factor on the right-hand side, it is a factor of the second. Thus, the degree of the minimal polynomial is at most two. Since, by (1), it is at least two, it must be equal to two (and $m(x) = x^2 + x + 1$). Thus

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{7}, \omega) : \mathbb{Q}(\sqrt[3]{7})][\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

By the above, $\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2\}$ is a basis of $\mathbb{Q}(\sqrt[3]{7})$ over $\mathbb{Q}$ and $\{1, \omega\}$ is a basis of $\mathbb{Q}(\sqrt[3]{7}, \omega)$ over $\mathbb{Q}(\sqrt[3]{7})$. By the Multiplication Theorem, a basis for E over $\mathbb{Q}$ is given by

$$\left\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2, \omega, \omega\sqrt[3]{7}, \omega(\sqrt[3]{7})^2\right\}.$$

QUESTION 11. Suppose $F \subseteq E$ is a field extension and $u, v \in E$.

(a) **[1 point]** Show that if $u - v \in F$, then $F(u) = F(v)$.

(b) **[2 points]** If $u^2 - v^2 \in F$, it is necessarily true that $F(u) = F(v)$? Remember to justify your answer.

Solution:

(a) Let $a = u - v \in F$. Then $v = u - a \in F(u)$, and so $F(v) \subseteq F(u)$. Similarly, $v = a + v \in F(v)$, and so $F(u) \subseteq F(v)$. Hence $F(u) = F(v)$.

(b) No, this is not true in general. For example, consider the field extension $\mathbb{Q} \subseteq \mathbb{C}$, with $u = \sqrt{2}$ and $v = \sqrt{-1}$. Then $u^2 - v^2 = 2 + 1 = 3 \in \mathbb{Q}$. However, $\sqrt{-1}$ is not real, and so is not contained in $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Thus $\mathbb{Q}(\sqrt{-1}) \neq \mathbb{Q}(\sqrt{2})$.

QUESTION 12.

(a) **[1 point]** Prove that $f(x) = x^3 + x^2 + x + 3 \in \mathbb{Z}_5[x]$ is irreducible.

(b) **[2 points]** Construct a field of order 125.

Solution:

(a) Since $f(x)$ has degree three, it suffices to check that it has no roots in $\mathbb{Z}_5$. We have

$$f(0) = 3, \quad f(1) = 1, \quad f(2) = 2, \quad f(3) = 2, \quad f(4) = 2.$$

Thus $f(x)$ has no roots in $\mathbb{Z}_5$ and thus it is irreducible.

(b) Since $f(x)$ is irreducible, the principal ideal $\langle f(x) \rangle \subseteq \mathbb{Z}_5[x]$ is maximal. Therefore, the quotient ring

$$\mathbb{Z}_5[x]/\langle f(x) \rangle$$

is a field. This field has basis $\{1, x, x^2\}$ over $\mathbb{Z}_5$, and so it has $5^3 = 125$ elements.